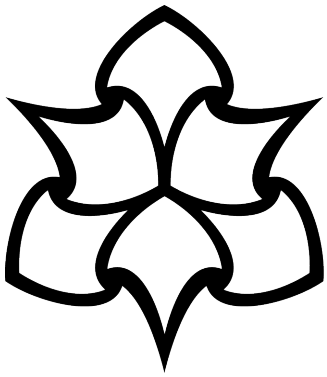

J Supercomput
https://doi.org/10.1007/s11227-018-2337-2

Security threats to critical infrastructure: the human factor

Ibrahim Ghafir[1,2] · Jibran Saleem[3] · Mohammad Hammoudeh[3] · Hanan Faour[4] · Vaclav Prenosil[2] · Sardar Jaf[1] · Sohail Jabbar[5] · Thar Baker[6]

Abstract In the twenty-first century, globalisation made corporate boundaries invisible and difficult to manage. This new macroeconomic transformation caused by globalisation introduced new challenges for critical infrastructure management. By

✉ Ibrahim Ghafir
ibrahim.ghafir@durham.ac.uk

Jibran Saleem
J.Saleem@mmu.ac.uk

Mohammad Hammoudeh
m.hammoudeh@mmu.ac.uk

Hanan Faour
h.faour@hbmsu.ac.ae

Vaclav Prenosil
prenosil@fi.muni.cz

Sardar Jaf
sardar.jaf@durham.ac.uk

Sohail Jabbar
sjabbar@ntu.edu.pk

Thar Baker
t.baker@ljmu.ac.uk

1 The University of Durham, Durham, UK

2 Masaryk University, Brno, Czech Republic

3 Manchester Metropolitan University, Manchester, UK

4 Hamdan Bin Mohammed Smart University, Dubai, UAE

5 National Textile University, Faisalabad, Pakistan

6 Liverpool John Moores University, Liverpool, UK

Published online: 26 March 2018

replacing manual tasks with automated decision making and sophisticated technology, no doubt we feel much more secure than half a century ago. As the technological advancement takes root, so does the maturity of security threats. It is common that today's critical infrastructures are operated by non-computer experts, e.g. nurses in health care, soldiers in military or firefighters in emergency services. In such challenging applications, protecting against insider attacks is often neither feasible nor economically possible, but these threats can be managed using suitable risk management strategies. Security technologies, e.g. firewalls, help protect data assets and computer systems against unauthorised entry. However, one area which is often largely ignored is the human factor of system security. Through social engineering techniques, malicious attackers are able to breach organisational security via people interactions. This paper presents a security awareness training framework, which can be used to train operators of critical infrastructure, on various social engineering security threats such as spear phishing, baiting, pretexting, among others.

Keywords Critical infrastructure security · Security awareness · Cyber security training · Work-based security training · Security threats against critical infrastructure

1 Introduction

Thanks to technology, our chances of survival have been drastically improved, in the event of an emergency. In fact, technology has positively improved how we live, how we travel, how we interact, how we learn, how we are medically treated and most importantly how we lead our lives. The technology used in critical infrastructure that supports our day to day life is becoming a necessity, without which life seems unimaginable. However, this necessity of life has also attracted a lot of interest from those who are illegally trying to gain access to personal, business or corporate data to satisfy their objectives. Many citizens fall victim to these attacks and suffer from minor to life-changing consequences. From losing access to personal photographs of sentimental value due to a ransomware attack to losing the custody of your children, the result of these attacks can mean life or death in some severe cases [1]. When these attacks are targeted towards critical infrastructure, the consequences can be even more devastating. Consider the case of ransomware attack on the NHS in May 2017 [2]. The attack resulted in a significant meltdown of emergency services in the UK. It is now being argued that the attack on NHS could have been prevented through due care, regular updates to NHS IT infrastructure and employee training [2]. However, the question is, how others critical infrastructure operators learned from this calamity and what they intend to do to avoid a similar situation?

With the emergence of smart cities, the opportunities of gain for malicious attackers have grown, along with their motivation. Great damage and substantial financial loss have been caused by malware, botnets [3,4] and targeted attacks [5,6] through deceiving the user to connect to malicious domains or websites [7,8]. Although intrusion detection systems [9] and monitoring tools [10,11] play a significant role in the network security, the human factor should be taken into consideration. It is imperative that due care and caution is taken at all level during interaction with technology to

ensure that users do not accidentally introduce malware to the organisation [12]. While security awareness training solutions have been known to provide effective mechanisms for learning and knowledge transfer on security measures, they suffer from few shortcomings. For instance, the monitoring aspect of the employees going through the training process may not be efficient nor effective. This lack of effectiveness occurs because in cases where critical organisations have large numbers of employees requiring awareness training, adequate progress monitoring is a monotonous task with a higher margin of error. Similarly, upon completion of the courses, most employees may have forgotten some of the knowledge and information related to security awareness, acquired earlier on in the training workshops. A recent research [13] found that after attending a business training session, employees, in general, tend to lose 50% of the information in an hour, 70% of the information is forgotten in twenty-four hours and 90% in a week. Thus, it is vital that awareness training is integrated into employees day to day tasks, to support retention and application of the knowledge acquired.

Other prevention aspects such as vulnerability assessment, physical security and the implementation of effective policies and procedures in critical infrastructure systems are equally as important as staff awareness training. To improve technical challenges and shortcomings faced by organisations, the proposed cyber defence strategy will focus on offering concise cyber incident prevention guide to organisations, who operate critical infrastructure. Our proposed cyber defence strategy will enable these organisations to protect their assets, as well as efficiently train their employees, so they are better prepared to deal with cyber and social engineering attacks. This paper proposes a context-aware education tool to be deployed in a business environment to raise the security awareness of the employees. The developed application utilises a client–server model, which can be configured by the administrator to set different modules to be presented according to the current user activity. Each module covers a specific aspect or topic related to security awareness in the business environment. In case the user activity does not trigger the application to display information, then the application autonomously selects tips and present them to the user. The administrator can also monitor the progress of each user while allowing for the setting of deadlines for completion of each module.

The remainder of this paper is organised as follows. Section 2 discusses the continuously growing threat of social engineering. Section 3 lists human traits, which are actively exploited by social engineers during an attack. Section 4 presents the current security awareness programmes in the market. The design and implementation of a proposed security awareness training programme is explained in Sect. 5. Section 6 shows the software testing and evaluation methodology. Section 8 concludes the paper.

2 Social engineering: a growing threat

In the recent years, organisations of all types and sizes, including those offering critical and emergency services, have been the victim of social engineering attacks [14]. As more organisations acquire enhanced IT solutions and robust encryption tools to protect their data, attackers will continue to resort to old-fashioned methods of exploiting human weaknesses, to achieve their objectives [15,16].

Social engineering is an ultimate psychological manipulation technique that is used by attackers to generate responses from unwilling targets, which are not in their best interest and coerce them into a position of disadvantage. This act is mostly conducted with the aim of influencing the other party to carry out actions, either lawful or unlawful, which may go against them, or others around them. The influence could be as simple as tricking an office employee to allow an actor into their workplace unchallenged, or it could be as complicated as obtaining state secrets through coercion, blackmail, manipulation, extortion or intimidation.

Today, social engineering is among the top information security threat faced by the multiple industries and organisations and thus far proven to be challenging to protect against [17–19]. The only practical protection available against social engineering attacks is cybersecurity awareness and training [20,21]. For instance, when a social engineering attack occurs, all the technical protection systems combined cannot stop an employee from giving out their password to an attacker over the phone. But with the appropriate security training, that same employee can act as the most reliable contender in the line of defence and alert relevant department about the social engineering attack attempt, potentially saving the company from a major security incident.

To develop an understanding of the security threats, it is essential to understand what social engineering manipulations techniques are used during an attack. This understanding can be achieved through experience, taught examples as well as training, like the one discussed in Sect. 4 of this paper. The knowledge acquired through a well-developed training framework will aid the trainees in gaining an understanding of social engineering attack strategies, as well as the ability to counter and limit any potential harm.

3 Social engineers attack strategies

Social engineers employ a variety of tactics to trap their targets into performing actions of their choice. It could be something as simple as gaining the trust of someone over the phone to get confidential information to the setup of bait for someone to access a compromised website via phishing methods. Social engineers are the modern equivalent of con artists, with the only difference that the latter uses non-technical methods to cheat people out of their hard-earned money.

Out of the many taxonomies and models available, Kevin Mitnick's social engineering attack cycle, as described in his book *The art of deception: controlling the human element of security* [22] is the most commonly recognised social engineering attack model. As illustrated in Fig. 1, the model depicts the four phases which occur before and during a social engineering attack.

During the *Research* stage, information is gathered about the target, its weaknesses and information that can aid the attacker during the later phases of the attack. *Develop Rapport and Trust* is the second stage of the attack during which the attacker aims to acquire trust of the target, which is later exploited during the third stage *Exploit Trust* to elicit information from the target, manipulation of the target or merely instructing the target to carry out actions in order to gain the desired knowledge or action. The fourth and last stage in the model *Utilise Information* is the final act of attack, during

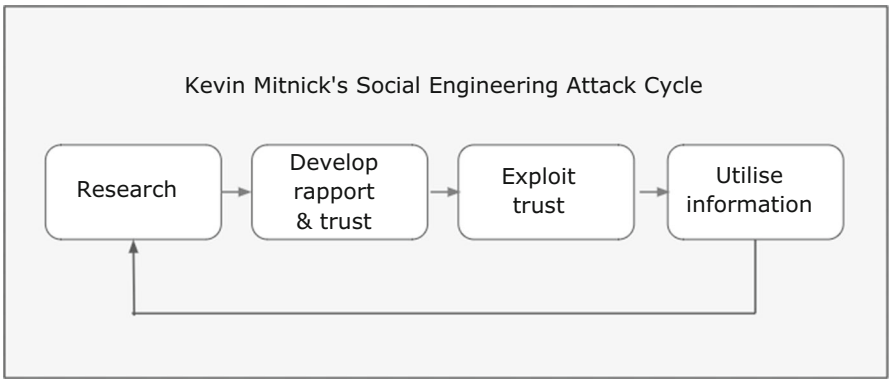

Fig. 1 Kevin Mitnick's social engineering attack cycle [22]

which information and resources acquired during the first three stages is put into action to get the desired result.

The next subsections will further examine which particular human traits are generally exploited by social engineers to force compliance from the subjects.

3.1 Psychological manipulation

In many cases, the usual target of a social engineering attack is someone who is in a position of authority, or at minimum be in possession of privileged information, which is useful for social engineers. For an employee to reach that level, they naturally have to go through certain steps within their company to prove their competence. Therefore, the majority of the people being exploited by the social engineers do have the expertise or reasonable proficiency, in their line of work. Yet, we see how easily social engineers fool people into handing over sensitive information [23].

Social engineers use various psychological manipulation techniques to acquire the confidence of their attack subjects. The methods they use vary from the usage of emotions, play on words, charm and impersonation to get the target to feel at ease with them.

3.2 Obedience to authority

Humans are wired to respect authority. From a young age, we are taught by the elders to give respect and listen to people in authority. This implies obeying parents, teachers, law, and when one enters a professional life, this extends to managers, bosses and superiors who demand that level of adherence. This is precisely another psychological vulnerability in humans, which social engineers so eagerly exploit.

Being respectful and courteous is important, but becoming exceptionally compliant when orders are issued from superiors is an unhealthy attitude with detrimental consequences and is indeed a psychological flaw in some people, which is actively exploited by social engineers.

3.3 Exploiting naivety

Social engineers thrive on people naivety. Once we take into account the fact that some people can be non-analytic, technology-ignorant, lack Internet usage experience and couple this with natural gullibility, we realise that those members of our society are publicly holding an "open to exploitation" placard in their hands.

Once a window of opportunity presents itself, social engineers act without any undue delay. Natural disasters, celebrity gossip news and trending topics is a popular way scammer attempt to grab the attention of their potential victims and tempt them to click on click-bait links. These links are then shared and spread across the Internet through compromised accounts. The idea usually is to get people to click on the links, which leads them to a malicious website that infects their computers with malware which obtains their login credentials, while at the same time using the profile of newly acquired victim to spread the scam further [24].

The trend in the enterprise to invest more in the technology, but not the people, usually turns in to regret once a breach occurs. A company can install ten different types of firewalls and intrusion detection systems to protect data, but these measures are ineffective in stopping someone from handing over their credentials to an attacker in a well-organised social engineering attack. However, training and awareness can play a crucial part in assisting people to realise how to react when they are being attacked.

The next section explains the proposed social engineering defence framework, which can be adopted by enterprises and businesses to reshape the workforce into competent guardians against social engineering threat.

4 Security awareness training delivery mod

The choice of learning medium is critical to the success of the learning process [25]. Currently, delivery of security awareness programmes is mainly through two broad modes, namely computer-based training and instructor-led training.

4.1 Computer-based training

According to the University of North Carolina, this channel for delivering security awareness training is the most attractive to training and IT managers [25]. It is based on a belief that organisations should embrace new technology where the learning medium is founded on the technology itself. There exists some computer-based training programmes or systems in the market such as SANS Online Security training, InfoSec Institutes, Global Learning Systems scenario-based system, among others.

The online course developed by SANS focuses on equipping employees with knowledge that can be used in securing their organisation's systems. It is delivered in the form of training videos with guided instructions. The programme is available in various languages and covers different organisational sectors including workforce working in the health care industry, engineers, developers and utility providers. Upon completion

of the course, the trainee has to go through an assessment which involves being tested on recognising phishing emails [26].

InfoSec's training programme delivers a highly interactive programme addressing compliance and security needs for logistics, manufacturing, retail, finance, government agencies and departments, educational institutions and consulting organisations. The training is delivered via interactive videos (short lectures) and exercises (realistic ones) that enable the learner to acquire hands-on experience in security awareness. Additionally, it provides customisable learning paths for each module and the ability to combine multiple modules [27].

Global Learning Systems also provide a comprehensive web-based security awareness training course, library and communication resources. The programme usually entails modules and courses that are scenario-based and can be deployed quickly. They are also customisable to provide an effective learning approach to the end user. It involves either 45-minute comprehensive or 20-minute short modules covering various topics. Besides the scenario-based learning approach, the programme also offers mini-challenges and quizzes [28].

Computer-based training programmes have several benefits, such as ease of delivery, reduced training costs, flexible learning structure and ongoing and easy access to information. However, these platforms also suffer from some drawbacks. The limitations include inadequate help or support on the training platform needed by the trainee to understand the topic thoroughly, unfamiliar learning environment, lack of mental stimulation for skilled trainees, non-customisable training programme and absence of formal accreditation such as CBT.

4.2 Instructor-led training

Instructor-led training is a preferred skill development choice of employers because it has been proven to be effective in behavioural development time and time again [29]. Instructor-led training is coordinated by the organisation where training schedules, workshops and events are arranged through a contracted trainer. This is mostly achieved by hiring experts in the area of systems security. Such a programme varies based on the organisational needs, allocated budget, number of employees and departments seeking training. For instance, employees in the IT department would require less security oriented training time than employees in the marketing department. Some of the companies which provide such training services include SANS, InfoSec Institute, AppSec Consulting, HITECH, NIST (National Institute of Standards and Technology), NCSA (The National Cyber Security Alliance), FTC (the Federal Trade Commission) and SCIPP International, among others.

Some of the benefits of utilising instructor-led training for security awareness programme include face to face interaction between trainer and trainee, real-time and direct feedback, enhanced learning experience in a group setting, personalised training and hands-on learning experience. However, a number of challenges and limitations also exist in this traditional approach. Instructor-led training is generally time-consuming and costly, learning pace is inflexible, content is delivered in large volumes with no individual considerations. Additionally, the learning experience is

significantly affected and influenced by trainer's teaching ability and generalised teaching methods can affect learners who may either be fast or slow at absorbing training content.

5 A social engineering defence framework for critical infrastructure operators

The proposed security awareness programme seeks to combine the advantages of computer-based and instructor-led training delivery approaches into a single hybrid system. It entails carrying out of situated learning, which involves the use of a computer-based training tool along with visits by a trainer who would be tasked with reinforcing the knowledge trainees gained during the computer-based learning session. Additionally, the visiting trainer would have the duty to communicate business specific examples and topics which are critical to the host organisation. Although the instructor training sessions would be short and intermittent, the training programme would continue via the computer-based tool with an integrated support mechanism. The authors made the developed software available to the public in [30].

6 Design and implementation

This section gives the design and development details of a context-aware, situational security awareness training framework. This framework uses a client–server model to allow the administrator to configure the security awareness content, organised in modules, to be presented to groups of users on different attack scenarios. Each training module covers a specific aspect or topic related to security awareness in the business environment. For example, the administrator can create a "Password Security" module to train users on how to choose secure passwords or how to manage their passwords.

When the user activity does not present a suitable context to trigger training content, the framework autonomously selects previously unseen educational subject matter and displays it to the user. The programme also allows the administrator to monitor the progress of each user and assign deadlines for the completion of each module. Upon completing a module, the user will receive a completion certificate in a digital format to their registered email account.

On the client side, the network integrated framework will monitor user's activity on their workstation and automatically present relevant, informative content in the form of pop-ups. For example, when a user visits Twitter or Facebook website, a pop-up screen will appear, displaying information on how to stay safe on social media.

The framework also provides external resources such as checking of password strength and offering additional information on technical topics. Once the pop-up screen appears, the user has several options including: "Remind me later", where the message will be displayed when the context is detected again, "Silence", which will put the application in sleep mode for a period specified by the administrator and Got it, which will mark the task as completed. Figure 2 shows the application flow diagram.

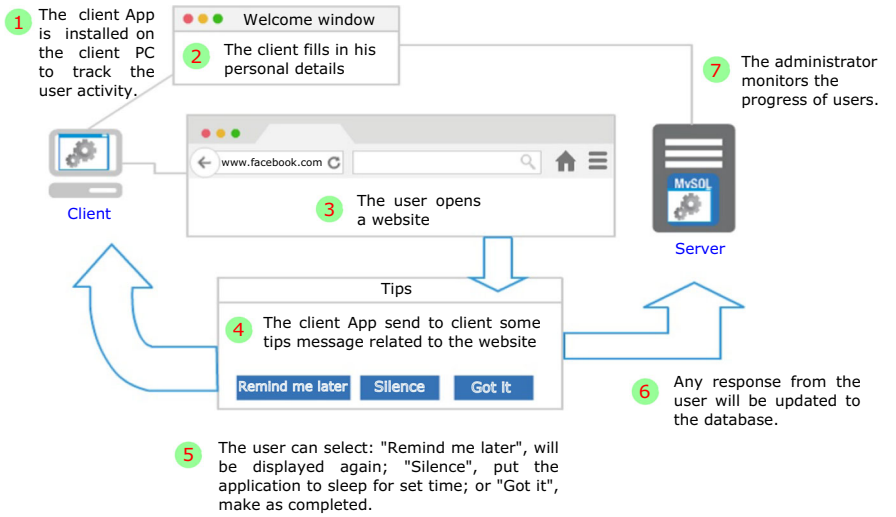

Fig. 2 Application flow diagram

6.1 Framework design

This section discusses two critical components of the proposed framework, namely database design and human interface design. Human interface design focuses on how information is captured from the users and how it is exhibited back to the users. Whereas database design is concerned with the physical and logical representation of the data requirements, the definition of data structures and transformation of the relationships into scientific databases and files [31].

The proposed framework has two interfaces, the administrator and the user. The administrator interface allows module and task creation, as well as activity monitoring. The user interface consists of context-specific content and options available to the user. User interface also contains a database component, which stores user's and modules information, e.g. personal details, completed modules, scores and time spent per activity.

This framework is an Internet-based application, which utilises TCP (transmission control protocol)-based client–server programming. Socket programming is a critical API (application programming interface) for programming Internet applications which are distributed [32].

The client–server model represents a widely used communication paradigm within networked systems. Clients usually communicate with one server, at any specific time. Whereas from the server side, a server can correspond with a number of clients at any given time. The client is required to know the server address, prior to connection, but this is not the case for the server. Communication is usually performed over several layers of network protocols.

In this research, the TCP (transmission control protocol) is used in providing a connection-oriented service for the client–server. The protocol is judged to be reliable,

as it requires acknowledgement from the server upon receipt of data. In the event of no response, the client is programmed to retransmits the data to the server [33].

6.2 Framework implementation

This section presents the implementation details of the proposed framework and explains its workflow. Through tracking the user activity, the framework selects content from the administrator configured module, which is related to the presented context. Additionally, based on the message options chosen by the user, the framework then provides further tips, tasks and modules subsequently. For instance, as a user tries to access a social media platform, such as Facebook, the framework identifies this activity and offers actionable options through a message pop-up. The machine-generated popups are influenced by historical tasks and modules, which are stored in the database.

When both the server and client are running successfully, a new window is displayed on the client PC titled "Personal Details". This window allows a user to connect to the application server via a login process for the already-registered users. There is also a registration option available for new users, who are not fully registered. The email address is unique to all users. Hence a user cannot sign on with the same email address more than once. After successful login into the system, the programme begins monitoring user activity. The application system is configured to focus on critical events such as credentials entry into websites, user browsing habits and even login into email accounts. For example, when a user logs into his Facebook account, the application will analyse and flag this activity and send a pop-up message to the user, containing information related to organisational policies on the use of social media.

Upon successful completion of all scheduled tasks, a user will be notified through a prompt that they have completed all the tasks. This message prompt will act as a confirmation to the user that all assigned training modules and activities are completed.

The context-content scoring algorithm of the proposed framework is based on Bayesian probability interpretations. The approach involves several operations. Firstly, random variables representing unknown quantities are used to model user activity, for a specified time period, then a prior probability distribution model is determined and applied to the collected variables. The third step involves the application of Bayes formula to the data for posterior distribution. Finally, a frequency probability is mapped out as either a one or a zero and applied to each user activity. Hence, generating a decision on whether or not to display a message.

The main question is how to autonomously personalise the developed application to the current user situation. The objective is to map the user activity to the best content to be displayed. To this end, the application collects data from two domains: users data and context data. Then, based on the current context a score is assigned to each "tip" in the tips repository. After that the application displays the tip of the highest score. The users data have information about name, age, gender, position, tasks, office hours and qualifications. The context data have information about the users activities such as browser history, running processes, used applications and login times. These data are used to build a profile for each user, and the probability of each attribute is calculated based on the frequency of each piece of data over the past period. The context

activities are classified into three levels of priorities: high, medium and low according to thresholds given to the computed probabilities. Based on this classification, the user can configure the number of tips generated by the application. The application monitors the users activities and each new activity is classified into a level of priority (high, medium or low) to decide whether a tip should be displayed. Afterwards, the Bayes rule is applied to calculate a score for each tip in the repository, as shown in Eq. 1.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{1}$$

where $P(A|B)$ is the tip score. $P(A)$ is the probability of the tip, computed based on the users data and tip level. $P(B)$ is the probability of the user activity, computed based on the frequency over the monitored period. $P(B|A)$ is an initial probability assigned by the administrator. Algorithm 1 shows the pseudo-code of the algorithm used for matching the user's activities into the displayed tips.

Algorithm 1 Implementation pseudo-code of matching the user's activities into the displayed tips

```
Get the set of tips
Get the set of user's activities
Calculate the user's activities probabilities over the past period
Classify the activities into levels of priority (high, medium and low)
for each new user activity do
    Classify the activity into a priority level
    if Priority level is high then
        Compute the score for each tip in the repository
        Display the tip of the highest score
        Update the user activity probability
    elsePriority level is medium or low
        Update the user activity probability
        Go to End
    end if
end for
End
```

6.3 Framework requirements

For the application to run:

1. The user machine must have jre 7 (Java Runtime Environment) or higher version installed on their machine.
2. In case jre is not installed, it can be downloaded via the JDK (Java Development Kit) [34].
3. For the database side, MySQL DBMS was used.

The programme consists of a server side and the client side application. The server side will run in the background and connect to the database, configured by the administrator. It will contain the following features:

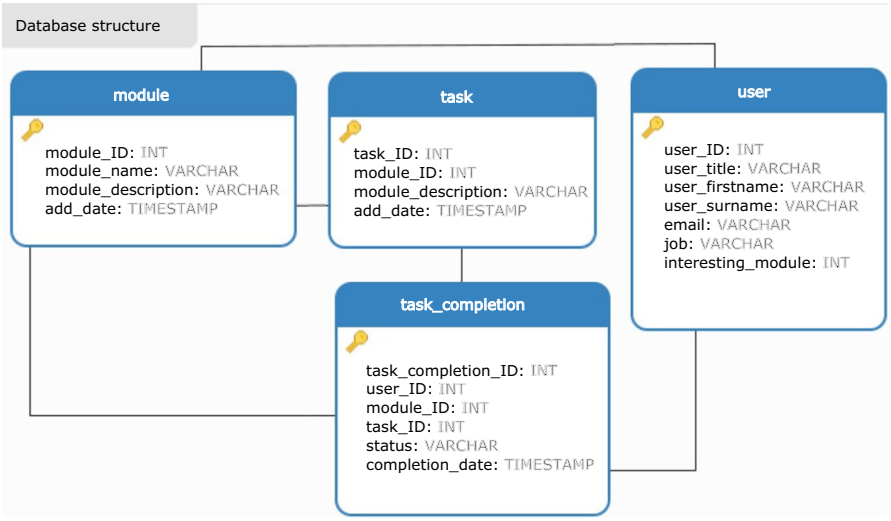

Fig. 3 Application database structure

- Configuration options for the user interface, which can be used by the administrator to manage the display of information to the user.
- A user interface that will be used by the administrator in creating, editing and updating tasks to be displayed as messages on the client side.
- Connection to the application database, illustrated in Fig. 3, allowing the administrator to monitor user progress, assign deadlines as well as overall management of the application.
- Management of user module and awarding of a completion certificate, in pdf format, upon successful completion of each task.

The client side runs on the user machine. It contains the following features:

- Creation of user account for first-time users, which will entail capture of user's details such as title, name, job title, email address. Additionally, they will also be presented with a selection of supplementary training modules they wish to complete.
- Receipt of pop message notification based on user activities on the PC. For instance, logging into a social media website will trigger a prompt on the system to display security awareness popup messages, related to the use of social media.
- Upon activation of awareness popup prompt, three options are displayed. Option 1, a Remind Me Later button, that postpones the notification to a later time, option 2, a Silence button, which puts the application to sleep for a specific time frame and option 3, a Got it button, which marks the task as completed.

7 Testing and evaluation

The testing and evaluation emphasises of this framework is on user experience and content accuracy. The following subsections present a set of experiments to measure these two critical design objectives.

7.1 Usability and user experience

Dialogue boxes or pop-ups are an effective tool to communicate information to the user and get them to respond. However, dialogue boxes temporarily interrupt user workflows. The first experiment is to evaluate user experience in terms of reading useful content, while being obstructed by an intransigent pop-up.

Thirty final year students studying humanities were given a laptop running the proposed framework. All participants were asked to perform the following tasks every ten minutes within one hour time interval: login to Facebook, login to email using installed software client, leave the machine idle for five minutes and execute an exe file. Each of these tasks triggers the framework to display a dialogue box with information related to the user context. At the end of the experiment, participants were asked on whether they felt that the framework was disruptive or not and why. The majority of the participants, 90%, responded that the dialogue boxes were not disruptive. Respondents highlighted that pop-ups were helpful to guide users through a potentially confusing process such as dealing with security warnings displayed when attempting to install a new application. Eight respondents found that the framework provided useful information to complete the task they were performing, particularly when faced with a situation where the user is required to confirm certain actions.

In regards to security, pop-ups proved to be an effective way of focusing user attention before irreversible actions are taken, e.g. enable a macro. User responses show that the proposed framework was successful in showing content while keeping the user on the same page within a reduced area. However, a small percentage of users found the framework to temporarily interrupt their workflows. They complained that they were forced to confirm an action at a critical time in the workflow.

Figure 4 shows the amount of time the users took before they dismissed the pop-up dialogue box. This reflects the level of user engagement with the framework. When interrupting users and diverting their navigation flow to a framework dialogue box relevant to their current context, none of the users dismissed the dialogue box without reading it. This can be justified by the offering of contextually appropriate topics that are based on the user's situation. The unitrusive nature of the framework allowed users to return their workflow to the original task after the pop-up appeared.

7.2 Accuracy

This experiment assesses the accuracy of the proposed Bayesian probability interpretations algorithm for the context-content matching. Three different users one month usage history database with sample size of 1000, 750 and 600, respectively, was used as a training database for the algorithm. The thirty participants were asked to rate the

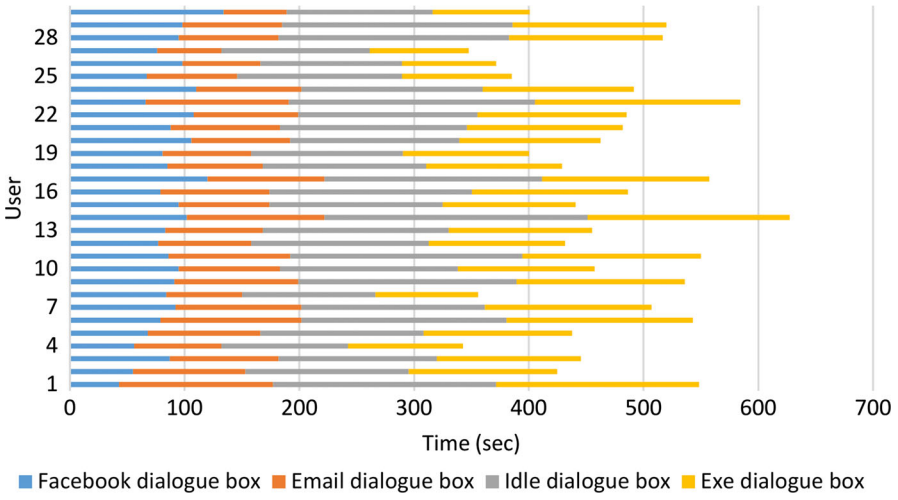

Fig. 4 Time before users dismiss a pop-up

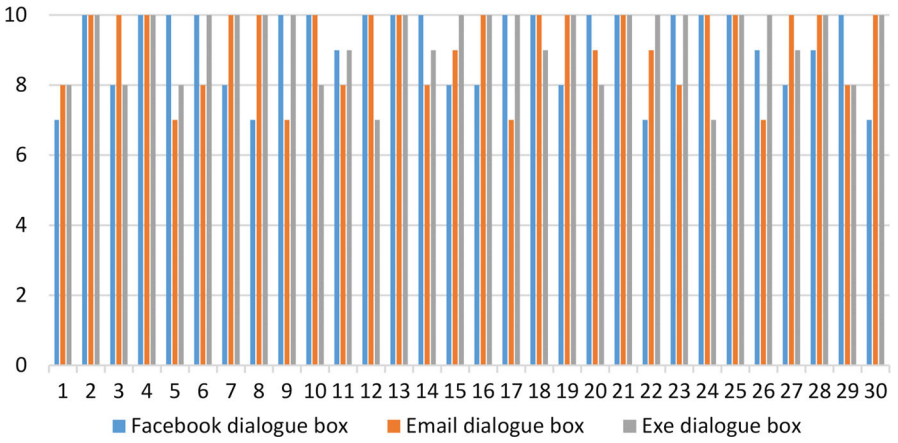

Fig. 5 Precision of content recommendation three different contexts

pop-ups content relevant to their current situation on a scale of 1 to 10. Most users agree that the precession rate was between 70 and 100. While the results in Fig. 5 show that this metric remains subjective, the participants responses on the precession of the content recommendation average to 91% which is acceptable by most applications.

The overall delay in calculating and displaying a recommendation is shown in Table 1. As described in Algorithm 1, the context-content matching involves several steps from context generation to the display of pop-ups actions (setting and services invocation). The overall delay to recommend a tip is calculated between 2.11 to 9 s.

Table 1 Recommendation overall delay

Activity	Time (s)
Context discovery	1–5
Rule matching	0.01–1
Setting adjustment	1–2
Service invocation	0.1–1

8 Conclusion and future work

This paper discusses the development of a security awareness training framework, which provides awareness tips to the end users within the business environment. In particular, the framework provides informative content to the employees regarding online security and social engineering, when users are logged on to their workstations and accessing websites which may lead to potential cyber attacks. This information presented to the users provides education relating to the dangers of social engineering attacks and the measures one can implement to protect personal and business data from potential loss.

The security awareness training programme has been developed to help businesses and employees so that they can gain an understanding of potential cyber hazards, as well as mitigating strategies available for self and business protection. The awareness training programme proactively monitors users activities and based on their usage, display informative messages in the form of window popups. These popups provide tips on various security topics and cyber issues. The training programme is also capable of monitoring user progress on administrator assigned awareness training modules. Additionally, the application also provides option for the organisations to set up specific deadlines for allocated training modules, introduce updated training content, configure existing modules and issue an achievement certificate, upon successful completion of all modules.

For future work, there are a number of functionalities that could be added to enhance user experience and knowledge. The improvements can include integration support for existing eLearning platforms, option to access assigned training modules at home or on personal portable devices with data synchronisation and accessibility features for disabled users. In addition, the algorithm that determines which data or tips are displayed, to the user, can also be enhanced to incorporate more factors and variables. This feature will improve the accuracy of the information presented to the user, based on their activity.

References

1. Saleem J, Adebisi B, Ruth A, Hammoudeh M (2017) A state of the art survey—impact of cyber attacks on SME's. p 52. https://doi.org/10.1145/3102304.3109812
2. BBC.co.uk (2017) NHS 'could have prevented' WannaCry ransomware attack. http://www.bbc.co.uk/news/technology-41753022. Accessed 15 Jan 2018
3. Ghafir I, Svoboda J, Prenosil V (2015) A survey on botnet command and control traffic detection. Int J Adv Comput Netw Secur 5(2):7580
4. Ghafir I, Prenosil V, Hammoudeh M (2015) Botnet command and control traffic detection challenges: a correlation-based solution. Int J Adv Comput Netw Secur 7(2):2731
5. Ghafir I, Prenosil V (2016) Proposed approach for targeted attacks detection. In: Advanced computer and communication engineering technology. Springer, p 7380
6. Ghafir I, Prenosil V (2014) Advanced persistent threat attack detection: an overview. Int J Adv Comput Netw Secur 4(4):5054
7. Ghafir I, Prenosil V (2015) DNS traffic analysis for malicious domains detection. In: 2nd International Conference on Signal Processing and Integrated Networks (SPIN). IEEE Xplore Digital Library, pp. 613–918
8. Ghafir I, Prenosil V, Hammoudeh M, Han L, Raza U (2017) Malicious SSL certificate detection: a step towards advanced persistent threat defence. In: Proceedings of the International Conference on Future Networks and Distributed Systems. ACM, p 27
9. Ghafir I, Husak M, Prenosil V (2014) A survey on intrusion detection and prevention systems. In: Proceedings of student conference Zvule, IEEE/UREL. Brno University of Technology, p 1014
10. Svoboda J, Ghafir I, Přenosil V (2015) Network monitoring approaches: an overview. Int J Adv Comput Netw Secur 5(2):88–93
11. Ghafir I, Prenosil V, Svoboda J, Hammoudeh M (2016) A survey on network security monitoring systems. In: IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE Xplore Digital Library, p 7782
12. Ghafir I, Prenosil V (2015) Blacklist-based malicious ip traffic detection. In: Global Conference on Communication Technologies (GCCT). IEEE Xplore Digital Library, pp. 229–233
13. Kohn Art (2014) Brain science: the forgetting curve–the dirty secret of corporate training. http://www.learningsolutionsmag.com/articles/1379/brain-science-the-forgetting-curvethe-dirty-secret-of-corporate-training. Accessed 15 Jan 2018
14. Ghafir I, Prenosil V, Alhejailan A, Hammoudeh M (2016) Social engineering attack strategies and defence approaches, In: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE Xplore Digital Library, pp. 145–149
15. Ubiquiti Networks, Inc (2015) Form 8-K. https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm. Accessed 15 Jan 2018
16. National Audit Office (2017) Investigation: WannaCry cyber attack and the NHS. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/. Accessed 15 Jan 2018
17. Jakobsson M (2018) Never mind malware—social engineering will be your biggest threat this year. https://www.infosecurity-magazine.com/opinions/social-engineering-biggest-threat/. Accessed 15 Jan 2018
18. Kilduff R (2018) 6 cyber security threats to watch for in 2018!. https://purplegriffon.com/blog/6-cyber-security-threats-2018. Accessed 15 Jan 2018
19. Ashford W (2016) Social engineering confirmed as top information security threat. http://www.computerweekly.com/news/4500273577/Social-engineering-confirmed-as-top-information-security-threat. Accessed 15 Jan 2018
20. Carella A, Kotsoev M, Truta TM (2017) Impact of security awareness training on phishing click-through rates. In: 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, pp. 4458–4466. https://doi.org/10.1109/BigData.2017.8258485
21. Bakhshi T (2017) Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors. In: 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, pp. 1–6. https://doi.org/10.1109/ICET.2017.8281653
22. Mitnick KD, Simon WL (2002) The art of deception: controlling the human element of security. Wiley, Indianapolis

23. Zetter K (2015) Teen who hacked CIA directors email tells how he did it. https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/. Accessed 15 Jan 2018
24. Chakraborty A, Paranjape B, Kakarla S, Ganguly N (2016) Stop clickbait: detecting and preventing clickbaits in online news media. In: 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, pp. 9–16. https://doi.org/10.1109/ASONAM.2016.7752207
25. Saleem J, Hammoudeh M (2018) Defense Methods Against Social Engineering Attacks. In: Computer and network security essentials, pp 603–618. https://doi.org/10.1007/978-3-319-58424-9_35
26. University of North-Carolina, Information security awareness training. https://its.uncg.edu/training/security/. Accessed 15 Jan 2018
27. Gulati R (2003) The threat of social engineering and your defense against it. SANS Reading Room
28. InforSec, Security awareness, http://resources.infosecinstitute.com/category/security-awareness/. Accessed 15 Jan 2018
29. Global Learning Systems, Employee security awareness training, http://www.globallearningsystems.com/products/security-awareness-training/
30. Security awareness framework (2018) https://www.dropbox.com/sh/plh7k38ahnruu6y/AACnVMCc9K1_yBB3Wi2eqMzca?dl=0
31. Payne S (2003) Developing security education and awareness programs. Educause Q 26(4):4953
32. Munassar NMA, Govardhan A (2010) A comparison between five models of software engineering. IJCSI 5:95101
33. Calvert KL, Donahoo MJ (2011) TCP/IP sockets in Java: practical guide for programmers. Morgan Kaufmann, Burlington
34. Oracle-Cloud, Java se development kit 7 downloads, http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html. Accessed 15 Jan 2018